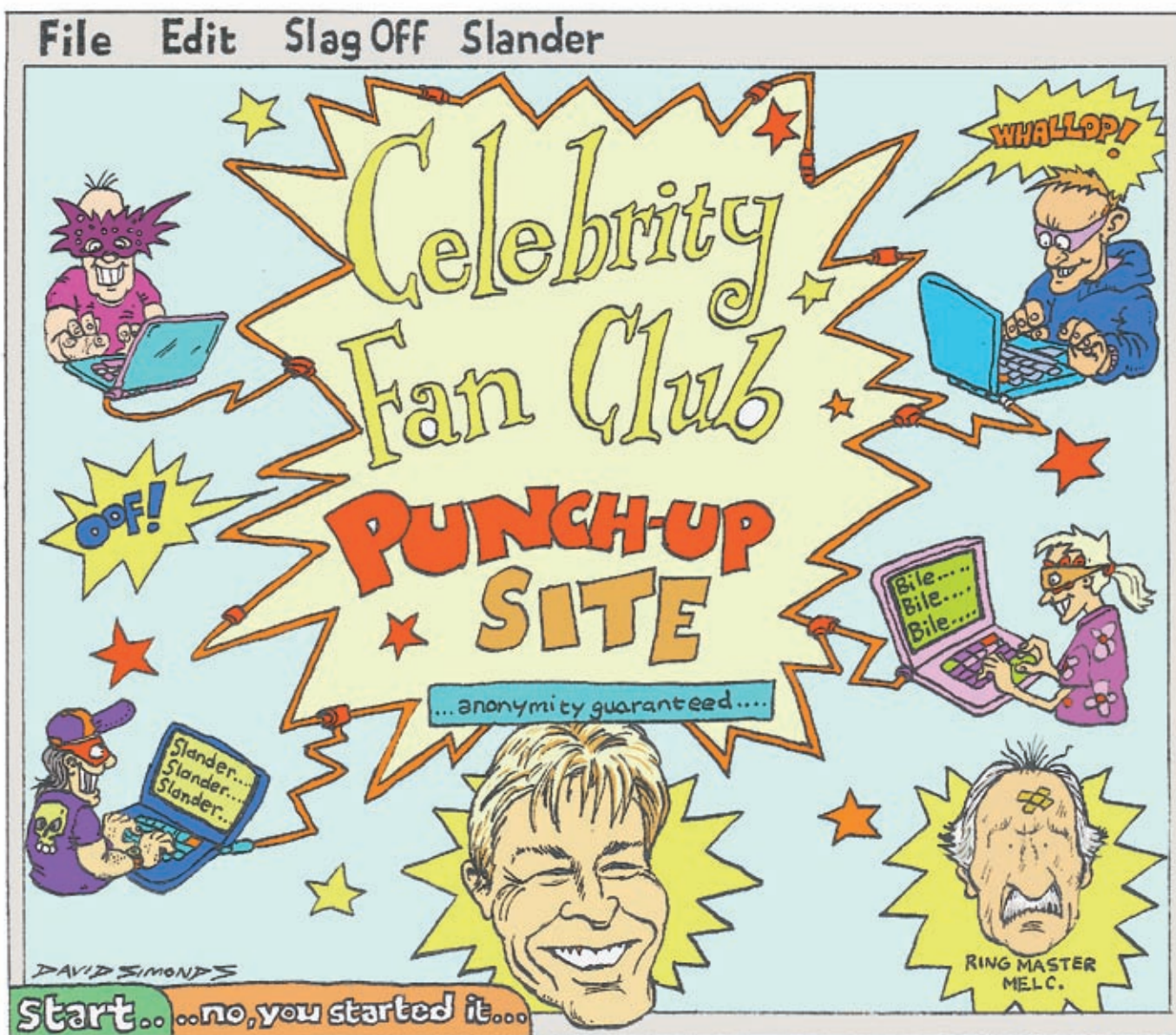




RANTS & RAVES

Mel Croucher finds that anonymous punch-ups and attempts to lure a film star into bed can't stop democracy online, while **Simon Edwards** finds you don't have to be stupid to get a virus

SEAN OF THE BED



MEL CROUCHER RAVES

I've been involved with celebrity websites for a long time. Among the galaxy of stars on my client list, I always thought of Sean Bean as my Polaris: at the centre of things and bright. But I wasn't very bright when I added a guestbook to the website for his Sharpe character, based on the works of Bernard Cornwell.

It launched without a hitch, and Sean Bean fans soon began posting their greetings, including numerous

offers to join him in bed. Then an online spat broke out over a trivial cinematographic detail, and the insults got nastier as more rabid types joined in the fray. Mayhem descended into chaos, and the guestbook was overwhelmed by scammers, spammers and legions of the deranged. There was nothing I could do about it, because our contributors masqueraded behind fictitious usernames. Every time someone got banned, they popped up again with a different name. Disgruntled employees slagged off their employers, peeved consumers railed against providers of shoddy

goods, children badmouthed their teachers and grown-ups wrote rude things about me. Some of which were quite untrue.

The reason individuals feel empowered to volunteer to go to bed with Sean Bean and attack the reputations of brands and individuals online is because they can lurk behind the cloak of false identity, free from all responsibility. An invitation to make up a username is asking to be abused.

The solution is obvious. Any online service or web-based facility worth a damn should insist that contributors identify themselves

correctly by a verifiable email address registered to the individual. By the same token, any contributor who feels they have something to say should be prepared to be identified and responded to electronically. There must be no exception to this, even when naming and shaming, grassing up criminals or declaring your love.

TOP TRIPS

And so I declare my own love for a new democracy that is sweeping through the web. I love websites and discussion boards that insist people identify themselves before they submit their opinion. My all-time favourite is tripadvisor.co.uk, offering indispensable information from real people about real places. I can safely ignore all the bumph put out by hoteliers, restaurateurs and purveyors of leisure services, because I can view candid photos of what's really on offer and read genuine experiences written by people who've been there, done that and signed their name. If



anyone should disagree, then the freedom is there to declare yourself and put an alternative viewpoint.

The ultimate expression of web democracy is Wikipedia.org, that global encyclopedia of everything, written and edited by anyone who feels like it. When I am very old and incapable of stringing a coherent page together, I intend to spend my last days correcting trivial errors on Wikipedia and making the world a better place before I depart it.

Until then, I applaud the new online transparency, and I even forgive Silas Minkey, Oscar The Cat and Zagrebo. These dubious identities are credited with writing the Wikipedia information about me that's currently online. I've got a suspicion that it's you, Sean, so put down that wench and identify yourself. You know you want to.

HACKED OFF



**SIMON EDWARDS
RANTS**

I was going to start off this article by railing against stupid PC users who deserve everything they get when surfing the internet. I intended to point out that people who visit free porn sites and download cracked software are massively increasing their chances of exposing their PC to spyware.

I was going to point to an article on the web (<http://tinyurl.com/25klcw>) that illustrates just how stupid some people are. It documents an experiment that involved creating a Google advert, which offered people a chance to have their PC infected with a virus – and it had punters clicking on it in their droves. My plan to criticise the idiots who make up most web users was scuppered when I read a research paper published by Google that gives a detailed view into the nasty underworld of spyware. This is software installed on your PC without your knowledge, or it pretends to do one thing but does other, usually harmful, tasks.

The reason this paper stopped me slagging off regular internet visitors is that it described how advanced the spyware-spreading hackers have become. It is seriously heavy reading. It is written in a formal, academic style and, like, the news it brings is heavy, man.

TRICK OR TREAT

Hackers have been reading the same security advice we've been passing on to concerned readers for the past few years. Now they have come up with ways to bypass the generally acknowledged hacker counter-measures. There has been

a shift from trying to trick users into clicking on things, and now hackers are taking more direct action – hijacking your system instead and forcing their spyware on to it without your knowledge.

For example, we once warned you not to click on unusual email attachments, particularly those sent by untrusted sources. Virus writers then came up with a way to launch infections when you opened an email to read it. That's not to say it's now OK to click on random attachments, but it does mean you shouldn't even open a suspect email if you want to avoid viruses. This is not a practical way to behave, so the bad guys win.

We once warned you to avoid the seedier parts of the web. Therein lie incredible temptations, including pirated software, naughty pictures and naughtier videos. One significant difference between internet porn and top-shelf magazines is that the only harm you can come to using the paper product is a slightly lowered sense of self-respect and a lighter wallet. Pink pixels have a greater impact.

The people who want to infect your PC with spyware no longer need you to make an active decision to download an attractive but illicit file, such as a screensaver of Paris Hilton nakedly gyrating or a licence key-generating program for Norton AntiVirus. Just visiting a site can cause you to lose control of the system while spyware is secretly installed.

Spyware creators still cater for 'clients' who want dodgy files, and will happily infect their systems in a trice. Likewise, attempting to view free pornography may result in a page that requires you to download some special viewer software, known as a codec. This is really spyware. But these so-called social engineering techniques are less popular than they used to be. You don't need to be stupid or naïve to catch a spyware infection. You just need to be online.

TRUST NO-ONE

Even visiting trusted sites can be a problem. Attackers are hacking popular websites and adding spyware to otherwise legitimate pages. Many sites let their users post comments and upload other content. Lots of these don't check thoroughly what the users upload or type, providing an opportunity for the bad guys to abuse the site, possibly directing visitors to places where their systems invisibly download spyware.

Advertising can provide a way for someone to serve spyware from a legitimate, popular site. The way online advertising works means

that, in some cases, a popular site might pass responsibility for the adverts that appear on its pages to another company. This company might be trustworthy, but it might subcontract some of the work to another. This may also subcontract and, before you know it, a chain of companies ends up managing the adverts. In documented cases, these chains have started with respectable companies but have ended up with spyware-spreading organisations. The result can be nasty code on legitimate websites. This code can force users' web browsers to download spyware automatically in the background.

Finally, hackers can create apparently useful pieces of software that can add extra features to a website. Third-party hit counters are an easy way for non-programmers to see how many people view their webpages. One minute these add-ons can be legitimate, handy tools; the next they may become privacy-invading spyware designed to compromise visitors to the site. If you run a website, even a small one, and use third-party add-ons that involve pasting special JavaScript into your pages, you are potentially putting your visitors at risk.

So that's the bad news: the world's collection of hackers are getting pushier and no longer need you to be a fathead who clicks any link coming your way. They'll come direct to you, thrusting infections in your (PC's) face. Unless you are very lucky, it will then suppurate your personal information.

This month, we've tested some popular anti-spyware software. If you check the results on page 119, you'll see that many well-known products fail to detect even close to 100 per cent of the bad files. This means if you install security software, keep your operating up to date and avoid bad sites, you still face the risk of spyware. The good news is you no longer have to blame yourself when that happens.

SAVE THE CHILDREN



**SIMON EDWARDS
RANTS**

I was amazed to wake up this morning to find that my brain had not steamed like a Christmas pudding and my face had not slid to the floor like a greasy fried egg. The reason I was so surprised not to wake up baked in bed is because I have a wireless network at home which, as we all know, is incredibly dangerous because it uses something called 'radiation'.

Radiation is invisible and wireless networks use it to move

data around without wires. In my book that makes it 'magic' and, as we all know, magic can be dangerous, particularly when it is invisible. It's pretty dangerous when it's green, like in sci-fi movies, but the unseen threat is always the spookiest.

I had not realised that WiFi radiation was dangerous, having considered that low-powered microwaves using this range of frequencies to be both incapable of heating water (such as you would find in human cells) and too feeble to penetrate more than a few millimetres of skin. But, you see, I was not thinking of the children.

Panorama thought of the kids, though. The BBC recently broadcast a documentary that investigated the levels of wireless networking radiation (that word again) in schools. Some schools were being bombarded by signals up to three times as strong as the radiation emitted by that well-known threat, the mobile phone mast. And we all know about mobile phones (except that we precisely don't). By the way, that massive level of radiation in schools is hundreds of times lower than the government's safety limits, but let's not forget that radiation is magic so the levels don't really matter as long as you can say they are higher than something that sounds vaguely threatening.

THIN IN THE HEAD

The problem is that children's skulls are thinner than those of adults. Adults' skulls can absorb more radiation, which means that less gets through to our brains. Read between the lines and you could believe that children, with their egg-shell craniums, are gamma-ray magnets, absorbing radiation like green-glowing sponges. That can't be good and someone should probably do something about it. Like make a documentary or write some news stories.

I am not a radiation expert, so I cannot engage in a proper scientific discussion about it. *Panorama* has an advantage here because it found some scientists who reckon there is a connection between something or other to do with radiation and another big scare-word: cancer.

I don't know who these guys are and, being a layman, I have never heard of the places where they work. And hey, they are talking about children, radiation and cancer. Only a fool would dismiss the *Panorama* investigation as a headline-grabbing exercise in fear, uncertainty and doubt. Destroy all wireless networks now. It's the only way to be sure. **CS**